PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-257668
(43)Date of publication of application : 21.09.2001

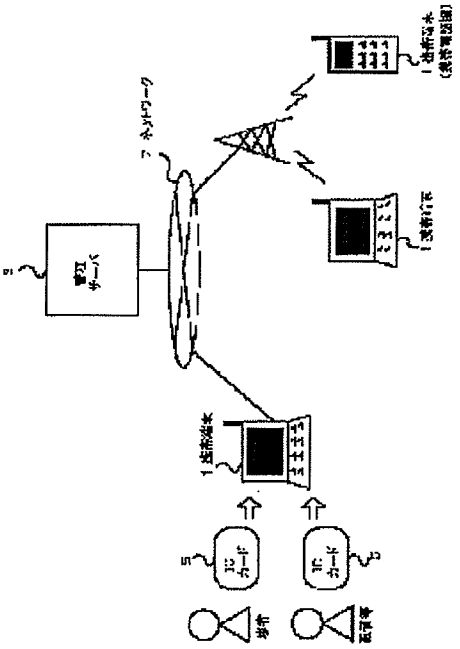
(51)Int.Cl. H04L 9/08
G06F 15/00
G06K 17/00
G06K 19/073
G09C 1/00
H04L 9/32

(21)Application number : 2000-069794
(22)Date of filing : 14.03.2000

(71)Applicant : NTT DATA CORP
(72)Inventor : NIIMURA TAKAHIKO
KOBAYASHI TAKAFUMI
MACHIDA OSAMU

(54) AUTHENTICATION SYSTEM, PORTABLE TERMINAL, CERTIFYING METHOD AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication system having high flexibility.
SOLUTION: An IC card 5 makes response to an access request from the other IC card 5 and obtains the authentication key (open key and the like) and access information of the IC card 5 being an access request source from a management server 3 managing the authentication keys and access information of all IC cards 5 through a terminal 1. The IC card 5 checks a signature from the access request source and an access instruction by using the obtained authentication key and access information. When a check result is normal, access from the other IC card 5 is permitted and the requested instruction is performed.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－257668
（P2001－257668A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/00	３３０Ｇ　５Ｂ０３５
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｋ　17/00	Ｅ　５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０８５
19/073			６６０Ａ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６０１Ｄ　９Ａ００１

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2000－69794(P2000－69794)

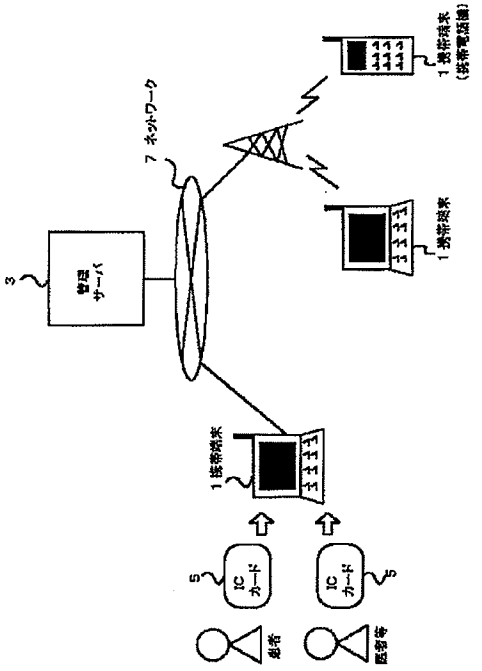
(22)出願日　平成12年３月14日(2000.3.14)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　新村　貴彦
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　小林　孝文
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

最終頁に続く

(54)【発明の名称】　認証システム、携帯端末、認証方法及び記録媒体

(57)【要約】
【課題】　柔軟性の高い認証システム等を提供することを目的とする。
【解決手段】　ＩＣカード５は、他のＩＣカード５からのアクセス要求に応答し、アクセス要求元のＩＣカード５の認証用鍵（公開鍵等）とアクセス情報を端末１を介して、全ＩＣカード５の認証用鍵とアクセス情報を管理する管理サーバ３から取得する。ＩＣカード５は、取得した認証用鍵とアクセス情報を用いて、アクセス要求元からの署名とアクセス命令をチェックする。チェック結果が正常である場合、他のＩＣカード５からのアクセスを許可し、要求された命令を実行する。



1

【特許請求の範囲】

【請求項１】各ＩＣカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第１のＩＣカードへアクセスを要求する第２のＩＣカードを認証するための認証システムであって、

携帯端末のカード処理部にセットされた第１のＩＣカードに対する第２のＩＣカードからのアクセス要求に応答して、前記第２のＩＣカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、

取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第２のＩＣカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第１のＩＣカードへのアクセスを許可する、

ことを特徴とする認証システム。

【請求項２】各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第１の携帯端末へアクセスを要求する第２の携帯端末を認証するための認証システムであって、

第１の携帯端末に対する第２の携帯端末からのアクセス要求に応答して、前記第２の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、

取得した認証用鍵とアクセス情報とを用いて前記第２の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第１の携帯端末へのアクセスを許可する、

ことを特徴とする認証システム。

【請求項３】前記携帯端末は、携帯電話機を含む、

ことを特徴とする請求項１又は２に記載の認証システム。

【請求項４】各ＩＣカードの認証に必要な認証情報を管理するセンタを備え、ＩＣカード間の認証を行うための認証システムであって、

各前記ＩＣカードは、

コンテンツ情報を記憶し、

他の前記ＩＣカードからのアクセス要求に応答して、当該他のＩＣカードの認証とアクセスレベルのチェックの少なくとも一方を含む認証処理行い、

前記認証処理の結果が正常を示す場合、コンテンツ情報へのアクセスを許可し、

前記センタは、

前記ＩＣカードに、認証処理に必要な情報を供給する、

ことを特徴とする認証システム。

【請求項５】アクセス要求元の認証を行う携帯端末であって、

他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得し、

2

取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可する、

ことを特徴とする携帯端末。

【請求項６】前記携帯端末は、携帯電話機を含む、

ことを特徴とする請求項５に記載の携帯端末。

【請求項７】各ＩＣカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第１のＩＣカードへアクセスを要求する第２のＩＣカードを認証するための認証方法であって、

携帯端末のカード処理部にセットされた第１のＩＣカードに対する第２のＩＣカードからのアクセス要求に応答して、前記第２のＩＣカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、

取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第２のＩＣカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第１のＩＣカードへのアクセスを許可する、

ことを特徴とする認証方法。

【請求項８】各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第１の携帯端末へアクセスを要求する第２の携帯端末を認証するための認証方法であって、

第１の携帯端末に対する第２の携帯端末からのアクセス要求に応答して、前記第２の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、

取得した認証用鍵とアクセス情報とを用いて前記第２の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第１の携帯端末へのアクセスを許可する、

ことを特徴とする認証方法。

【請求項９】コンピュータを、アクセス要求元の認証を行う携帯端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該コンピュータを、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得する手段、

取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセス

を許可する手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカード等へのアクセス管理を行うための認証システム等に関する。

【０００２】

【従来の技術】近年、情報技術の進歩により、各利用者が自己のＩＣカードを用いてサービスを受けることができるシステムが考案されている。これらのシステムでは、ＩＣカードへの不正なアクセスを防止するために、アクセス要求元の正当性やアクセス権限等をチェックしていた。例えば、アクセス要求元のチェックでは、アクセス要求元から、そのアクセス要求元の秘密鍵等でなされた署名等をＩＣカードが受け取り、相手の公開鍵を用いて署名の正当性をチェックしていた。

【０００３】また、アクセス権限のチェックでは、各ＩＣカードにそれぞれ付与されているアクセス権限の情報を参照して、アクセス要求元からのアクセス命令が、適正なアクセス命令であるかをチェックしていた。例えば、あるＩＣカードに、「Ａデータ」へのアクセス権限として、データの読出のみが許可されている他のＩＣカードから、データの書込を要求するアクセス要求を受信した場合には、アクセス権限外のアクセス命令であるとして、アクセスを拒否していた。

【０００４】

【発明が解決しようとする課題】上記のような認証システムでは、各ＩＣカード等は、アクセス要求元の認証を行うために、システムの利用者の全てのＩＣカードの認証用鍵とアクセス権限を示すアクセス情報とを保持しなければならない。しかし、各ＩＣカードにおいて、これらの情報を全て記憶させることは実質上困難であった。このため、メモリに記憶される認証用鍵とアクセス情報のデータが制限されるため、結果的に、サービス内容や利用者数など、システムの利用に関して種々の制限が課されていた。また、ＩＣカードに記憶される認証用鍵やアクセス情報が不正利用されないように、各カードの安全性等の機能を強化する必要があった。

【０００５】本発明は、上述した事情に鑑みてなされたもので、ＩＣカードの記憶容量に基づくシステムの利用制限を軽減することができる認証システム等を提供することを目的とする。また、本発明は、ＩＣカードの機能負担を軽減しつつ、システムの安全性を保持することができる認証システム等を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点に係る認証システムは、各ＩＣカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第１のＩＣカードへアクセスを要求する第２のＩＣカードを認証するための認証システムであって、携帯端末のカード処理部にセットされた第１のＩＣカードに対する第２のＩＣカードからのアクセス要求に応答して、前記第２のＩＣカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第２のＩＣカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第１のＩＣカードへのアクセスを許可する、ことを特徴とする。

【０００７】このような構成によれば、例えば全ＩＣカードの認証用鍵等をサーバで集中管理して、あるＩＣカードにアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、ＩＣカードに大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるＩＣカード側の負担を軽減することができる。

【０００８】また、本発明の第２の観点に係る認証システムは、各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備え、第１の携帯端末へアクセスを要求する第２の携帯端末を認証するための認証システムであって、第１の携帯端末に対する第２の携帯端末からのアクセス要求に応答して、前記第２の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報とを用いて前記第２の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第１の携帯端末へのアクセスを許可する、ことを特徴とする。

【０００９】このような構成によれば、例えば全携帯端末の認証用鍵等をサーバで集中管理して、ある携帯端末にアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、多数の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるＩＣカード側の負担を軽減することができる。

【００１０】また、第１と第２の観点に係る認証システムにおいて、前記携帯端末は、携帯電話機を含んでもよい。

【００１１】また、本発明の第３の観点に係る認証システムは、各ＩＣカードの認証に必要な認証情報を管理するセンタを備え、ＩＣカード間の認証を行うための認証システムであって、各前記ＩＣカードは、コンテンツ情

報を記憶し、他の前記ＩＣカードからのアクセス要求に応答して、当該他のＩＣカードの認証とアクセスレベルのチェックの少なくとも一方を含む認証処理行い、前記認証処理の結果が正常を示す場合、コンテンツ情報へのアクセスを許可し、前記センタは、前記ＩＣカードに、認証処理に必要な情報を供給する、ことを特徴とする。

【００１２】また、本発明の第４の観点に係る携帯端末は、アクセス要求元の認証を行う携帯端末であって、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可する、ことを特徴とする。

【００１３】前記携帯端末は、携帯電話機を含んでもよい。

【００１４】また、本発明の第５の観点に係る認証方法は、各ＩＣカードの認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第１のＩＣカードへアクセスを要求する第２のＩＣカードを認証するための認証方法であって、携帯端末のカード処理部にセットされた第１のＩＣカードに対する第２のＩＣカードからのアクセス要求に応答して、前記第２のＩＣカードの認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報との少なくとも一方を用いて前記第２のＩＣカードからの署名とアクセス命令をチェックし、チェック結果が正常を示す場合に、前記第１のＩＣカードへのアクセスを許可する、ことを特徴とする。

【００１５】このような構成によれば、例えば全ＩＣカードの認証用鍵等をサーバで集中管理して、あるＩＣカードにアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、ＩＣカードに大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるＩＣカード側の負担を軽減することができる。

【００１６】また、本発明の第６の観点に係る認証方法は、各携帯端末の認証用鍵とアクセス権限を示すアクセス情報との少なくとも一方を記憶するサーバを備えるシステムにおける、第１の携帯端末へアクセスを要求する第２の携帯端末を認証するための認証方法であって、第１の携帯端末に対する第２の携帯端末からのアクセス要求に応答して、前記第２の携帯端末の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、通信を介して前記サーバから取得し、取得した認証用鍵とアクセス情報とを用いて前記第２の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、前記第１の携帯端末へのアクセスを許可する、ことを特徴とする。

【００１７】このような構成によれば、例えば全携帯端末の認証用鍵等をサーバで集中管理して、ある携帯端末にアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、多数の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるＩＣカード側の負担を軽減することができる。

【００１８】また、本発明の第７の観点に係る記録媒体は、コンピュータを、アクセス要求元の認証を行う携帯端末として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、他の携帯端末からのアクセス要求に応答し、アクセス要求元の認証に必要な認証用鍵とアクセス情報との少なくとも一方を、各携帯端末の認証用鍵とアクセス情報との少なくとも一方を記憶するサーバから通信により取得する手段、取得した認証用鍵とアクセス情報との少なくとも一方を用いて、他の携帯端末からの署名とアクセス命令との少なくとも一方をチェックし、チェック結果が正常を示す場合に、他の携帯端末からの当該携帯端末へのアクセスを許可する手段、として機能させるためのプログラムを記録する。

【００１９】

【発明の実施の形態】以下、本発明に係る実施の形態を、病院等で使用されるＩＣカード認証システムを例に図面を参照して説明する。

【００２０】本実施形態に係るＩＣカード認証システムのシステム構成図を図１に示す。図示されるように、本システムは、携帯端末１と管理サーバ３とＩＣカード５と、を備え、携帯端末１と管理サーバ３は、例えば公衆回線網等のネットワーク７に接続される。

【００２１】携帯端末１は、ＩＣカード５間のデータの授受、ＩＣカード５と管理サーバ３とのデータの授受等を行うための装置であり、例えば図２に示すように、制御部１１と、カードリーダライタ部１３と、記憶部１５と、通信制御部１７と、を備える。

【００２２】制御部１１は、カードリーダライタ部１３に装着されているＩＣカード５と、他のＩＣカード５との間の情報の授受を制御等する。具体的には、制御部１１は、カードリーダライタ部１３に装着されているＩＣカード５へのアクセス要求等を他のカードから受信した場合には、そのアクセス要求等をＩＣカード５に送信する。例えば、カード挿入口を２つ備えるカードリーダラ

イタ部１３にそれぞれＩＣカード５が挿入され、一方のＩＣカード５からのアクセス要求を受信して、他方のＩＣカード５に送信してもよい。また、他の携帯端末１のカードリーダライタ部１３にセットされたＩＣカード５からのアクセス要求をネットワーク７等を介して受信して、自己のカードリーダライタ部１３にセットされているＩＣカード５に渡してもよい。

【００２３】また、制御部１１は、カードリーダライタ部１３に装着されているＩＣカード５から受信した種々の要求（検証情報要求、権限変更要求等）をネットワーク７を介して管理サーバ３に送信し、これらに対して管理サーバ３から送信されてくる情報を受信して、ＩＣカード５に送信する。

【００２４】カードリーダライタ部１３は、ＩＣカード５のデータの読取及び書込を行う。記憶部１３は、他の携帯端末１又は管理サーバ３から受信した情報を記憶する。通信制御部１５は、他の携帯端末１又は管理サーバ３とのデータ通信を制御する。

【００２５】なお、携帯端末１は、上記機能を備える携帯電話機、ＰＤＡ（Personal Digital Assistants）等を含む。

【００２６】管理サーバ３は、本システムの利用者の公開鍵やアクセス権限を示すアクセス権限表等を管理するコンピュータであり、図３に示すように、記憶部３１と、制御部３３と、通信制御部３５と、を備える。

【００２７】記憶部３１は、本システムの全利用者のＩＣカード５の公開鍵と、管理サーバ３の秘密鍵及び公開鍵と、アクセス権限表と、を記憶する。本システムでは、各利用者は、例えば「医者」、「薬剤師」等の所定のグループに分類されており、所属するグループを特定するためのグループＩＤが付与されている。なお、本実施例では、「医者」のグループＩＤを「ＧＩＤ１０」、「薬剤師」のグループＩＤを「ＧＩＤ２０」とする。

【００２８】アクセス権限表は、例えば図４に示すように、後述するＩＣカード５に記憶される個人情報の各データ（名前情報、住所情報、カルテ情報、処方箋情報等）について、それぞれのアクセス権限がグループＩＤ毎に設定されている。例えば図４に示すアクセス権限表には、名前情報及び住所情報については、医者と薬剤師による読み出し可能であることが設定されており、カルテ情報及び処方箋情報については、医者による読み出し及び書き込みが可能であることが設定されている。なお、このアクセス権限表は、例えばシステム管理者により入力設定される。

【００２９】制御部３３は、携帯端末１から、検証情報要求としてユーザＩＤとグループＩＤを受信すると、受信したユーザＩＤに対応する公開鍵を記憶部３１から読み出し、また、受信したグループＩＤに対応するアクセス情報を記憶部３１におけるアクセス権限表から読み出す。そして、読み出した公開鍵及びアクセス情報に、管理サーバ３の秘密鍵を用いた署名を付与して要求元の携帯端末１に送信する。

【００３０】また、制御部３３は、携帯端末１から権限変更要求を受信すると、記憶部３１に記憶されているアクセス権限表から読み出した情報に、指定された変更を施したアクセス情報を要求元に送信等する。この際、記憶部３１に記憶されているアクセス権限表の内容には何ら変更を加えない。権限変更要求には、所定グループのアクセス権限の追加を要求する権限追加要求と、所定グループのアクセス権限の削除を要求する権限削除要求と、新たなグループについてアクセス情報の登録を要求する登録要求等がある。

【００３１】権限追加要求は、変更対象グループのグループＩＤと、追加対象のコマンド（例えば、「カルテ情報を読出す」）と、を含む。制御部３３は、この権限追加要求を受信した場合、受信したグループＩＤのアクセス情報を記憶部３１のアクセス権限表から所定の記憶領域にコピーし、コピーされたアクセス情報に、受信したコマンドを追加する処理を行う（該当するデータ種別が「読出可」であることを設定する）。そして、コマンドが追加されたアクセス情報に管理サーバ３の秘密鍵を用いた署名を付して、要求元の携帯端末１に送信する。

【００３２】また、権限削除要求は、変更対象グループのグループＩＤと、削除対象のコマンドと、を含む。制御部３３は、この権限削除要求を受信した場合、受信したグループＩＤのアクセス情報を記憶部３１のアクセス権限表から所定の記憶領域にコピーし、コピーされたアクセス情報に、受信したコマンドを削除する処理を行う。そして、コマンドが削除されたアクセス情報に管理サーバ３の秘密鍵を用いた署名を付して、要求元の携帯端末１に送信する。

【００３３】また、登録要求は、登録対象のグループＩＤと、登録対象のコマンドと、を含む。制御部３３は、この登録要求を受信した場合、受信したグループＩＤについてアクセス情報を作成し、これに管理サーバ３の秘密鍵を用いた署名を付して、要求元の携帯端末１に送信する。

【００３４】なお、ＩＣカード５が管理サーバ３に所定の権限変更のための書換命令発効依頼を送信し、管理サーバ３がこれに応じた書換命令をＩＣカード５に送信し、これに応じて、ＩＣカード５が自己の保持するアクセス情報を書き換えるようにしてもよい。

【００３５】また、制御部３３は、携帯端末１からアクセス権限表の参照要求を受信すると、記憶部３１に記憶されているアクセス権限表に格納されているアクセス情報を読み出して、管理サーバ３の署名を付与して要求元の携帯端末１に送信する。また、参照要求とともに参照対象のグループＩＤを受信した場合には、制御部３３は、指定されたグループＩＤに対応するアクセス情報を読み出して要求元の携帯端末１に送信する。また、通信

制御部３５は、各携帯端末１とのデータ通信を制御する。

【００３６】ＩＣカード５は、本システムの利用者がそれぞれ保持するカードであり、ＭＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等を有するＩＣチップを備える。ＩＣチップは、例えば図５に示すように、ＭＰＵがＲＯＭ等に記憶されるプログラムを実行することにより実現される制御部５１とメモリ５２と入出力制御部５３とを備える。

【００３７】制御部５１は、そのＩＣカード５へのアクセスが要求された場合に、アクセス要求元である相手の認証及びアクセス権限の検証等を行う。この認証処理では、制御部５１は、まず携帯端末１を介して他のＩＣカード５からのアクセス要求を受信する。アクセス要求は、例えばアクセス要求元である相手のユーザＩＤとグループＩＤとアクセスコマンド等を含む要求情報と、署名等を含む。なお、この実施例でのアクセスコマンドとは、アクセス要求元が要求するアクセスの種別を示し、例えば「カルテ情報を読み出す」、「処方箋情報を書き込む」等のコマンドを示す。

【００３８】次に、制御部５１は、受信したアクセス要求における要求情報に含まれるユーザＩＤとグループＩＤについて、これらを含む検証情報要求を生成し、携帯端末１を介して管理サーバ３に送信する。そして、これに応答して管理サーバ３から送信されてくる検証情報（アクセス要求元の公開鍵とアクセス情報を含む）を携帯端末１から受け取ってメモリ５２に記憶する。

【００３９】制御部５１は、管理サーバ３から取得したアクセス要求元の公開鍵を用いて、アクセス要求における署名を復号化し、復号化結果が要求情報と合致するかを判別する等して、アクセス要求元の正当性をチェックする。

【００４０】また、制御部５１は、アクセス要求元のグループＩＤに基づいて、該当するグループＩＤのアクセス情報を参照し、アクセスが要求されているデータについて、要求されたコマンドの実行が許可されているか否かを判別する。例えばグループＩＤ「ＧＩＤ１０」の要求元から受信した「カルテ情報を読出す」というアクセスコマンドを検証する場合には、制御部５１は、グループＩＤ「１０」のアクセス情報を参照し、「カルテ情報」についての権限が「読出可」であることをチェックする。

【００４１】そして、署名の認証とアクセスコマンドの検証が正常に完了すると、制御部５１は、アクセス要求元からのアクセスコマンドを実行する。アクセスコマンドが例えば「カルテ情報を読出す」等の所定情報の読出命令である場合、制御部５１はメモリ５２から指定された情報を読み出し、携帯端末１を介してアクセス要求元のＩＣカード５に送信する。また、アクセスコマンドが例えば「処方箋情報を書き込む」等の所定情報の書込命令である場合、制御部５１は、その命令とともに受信した所定情報をメモリ５２に記録する。

【００４２】また署名の認証結果がエラーとなった場合、又は、アクセスコマンドの検証がエラーとなった場合には、制御部５１は、所定のエラー信号をアクセス要求元のＩＣカード５に携帯端末１を介して送信する。

【００４３】また、制御部５１は、そのＩＣカード５の保持者（利用者）からの要求に応じて、所定グループのアクセス権限の変更を管理サーバ３に要求するアクセス権限変更処理を行う。このアクセス権限変更処理では、制御部５１は、例えばＰＩＮの入力チェックにより本人確認を行ったのち、利用者から入力された、変更内容（権限の追加、権限の削除、新規登録等）と、変更対象のコマンド（追加、削除、登録等）と、変更対象グループのグループＩＤ等を携帯端末１から受け取る。そして、その入力データに応じて、グループＩＤとコマンドを含む権限変更要求（権限追加要求、権限削除要求、登録要求等）を作成し、携帯端末１を介して管理サーバ３に送信する。そして、この権限変更要求に応答して管理サーバ３から送信されてきた変更後のアクセス情報をメモリ５２に記憶する。なお、このアクセス情報の変更は、管理サーバ３の記憶部３１に記憶されているアクセス情報には反映されない。

【００４４】また、制御部５１は、そのＩＣカード５の保持者からの要求に応じて、管理サーバ３で管理されているアクセス権限表の参照要求を送信する。制御部５１は、アクセス権限表に格納されている全アクセス情報を要求してもよく、また、カード保持者からの１又は複数のグループＩＤの入力を受けて、入力されたグループＩＤに対応するアクセス情報の参照を管理サーバ３に要求してもよい。制御部５１は、この参照要求に応答して管理サーバ３から受信したアクセス情報を例えば携帯端末１を介して表示する。

【００４５】また、制御部５１は、他のＩＣカード５へアクセス要求を送信するアクセス要求処理を行う。制御部５１は、アクセスコマンドと、自己のユーザＩＤ及びグループＩＤを含む要求情報に自己の秘密鍵を用いた署名を付与したアクセス要求を生成し、アクセス要求先のＩＣカード５に対して発信する。

【００４６】メモリ５２は、例えば、図６（Ａ）に示すような、そのＩＣカード５に付与された秘密鍵及び公開鍵、ユーザＩＤ、グループＩＤ、管理サーバ３の公開鍵等の初期情報と、例えば図６（Ｂ）に示すような、カード保持者の個人情報（例えば、名前情報、住所情報、カルテ情報、処方箋情報等）等を記憶する。また、メモリ５２は、例えば図７（Ａ）に示すように、管理サーバ３から取得した認証相手先の公開鍵をユーザＩＤとともに記憶し、また、図６（Ｂ）に示すように、管理サーバ３から取得したアクセス情報をグループＩＤ毎に記憶する。

【００４７】各ＩＣカード５の秘密鍵及び公開鍵は、例えば各ＩＣカード５が、カード内で自己用の秘密鍵及び公開鍵を生成し、そのうちの公開鍵を携帯端末１を介して管理サーバ３に登録する。また、管理サーバ３が、各ＩＣカード５について秘密鍵及び公開鍵を生成し、そのうちの秘密鍵を格納した記録媒体を各利用者に配布してもよい。また、秘密鍵を暗号化して、通信により携帯端末１を介して各ＩＣカード５に送信してもよい。

【００４８】入出力制御部５３は、携帯端末１とのデータ通信を制御する。

【００４９】次に、本システムの動作について、ＩＣカード５間の通信及びＩＣカード５と管理サーバ３との通信を中心に、例えば患者Ａが病院に行って医者Ｂの診察を受け、診察後、薬剤師Ｃから薬をもらう場合を例に説明する。

【００５０】本システムでは、医者Ｂが患者ＡのＩＣカード５Ａにアクセスして、カード内に記憶されているカルテ情報を読むためには、医者ＢのＩＣカード５Ｂが患者ＡのＩＣカード５Ａによる認証を受ける必要がある。このカルテ情報を読むための認証処理について図８を参照して説明する。

【００５１】まず、患者Ａは、自己のＩＣカード５Ａを、例えば携帯端末１の第１のカード挿入口にセットする。また、医者Ｂは、自己のＩＣカード５Ｂを、携帯端末１の第２のカード挿入口にセットし、例えば相手（患者Ａ）のＩＣカード５Ａに記憶されているカルテ情報を見ることの要求を入力する。このときの入力方法は任意であり、医者が「カルテ情報を見る」というコマンドを直接入力してもよく、また、医者のアクセス権限を示すアクセス情報を携帯端末１が管理サーバ３から取得して表示し、その中から選択させてもよい。携帯端末１は、入力（又は選択）された「カルテ情報を読み出す」というアクセスコマンドを医者ＢのＩＣカード５Ｂに送信する。

【００５２】これに応答して、ＩＣカード５Ｂは、アクセスコマンド「カルテ情報を読み出す」と、例えばメモリ５２から読み出した医者ＢのユーザＩＤ「ＵＩＤ１」及びグループＩＤ「ＧＩＤ１０」を含む要求情報を生成し、また、この要求情報と自己の秘密鍵ＫＥＹＳ１を用いて署名を生成する。署名の生成方法は任意であり、例えば要求情報のハッシュ値を秘密鍵で暗号化して生成してもよい。そして、ＩＣカード５Ｂは、生成した要求情報に署名を付与したアクセス要求Ｓ１を、患者ＡのＩＣカード５Ａに携帯端末１を介して送信する（Ｌ１）。

【００５３】患者ＡのＩＣカード５Ａは、ＩＣカード５Ｂからのアクセス要求Ｓ１を受信する。ＩＣカードＡは、例えばアクセス要求Ｓ１における要求情報に含まれるユーザＩＤ「ＵＩＤ１」に対する公開鍵と、グループＩＤ「ＧＩＤ１０」に対するアクセス情報とが未取得であることをメモリ５２を参照して確認した後、ユーザＩＤ「ＵＩＤ１」とグループＩＤ「ＧＩＤ１０」を含む検証情報要求を、携帯端末１を介して管理サーバ３に送信する（Ｌ２）。

【００５４】管理サーバ３は、受信したユーザＩＤ「ＵＩＤ１」に対応する公開鍵「ＫＥＹＰ１」と、受信したグループＩＤ「ＧＩＤ１０」に対応するアクセス情報と、を記憶部３１からそれぞれ読み出し、これらの情報に、管理サーバ３の秘密鍵ＫＥＹＳＣＡを用いて生成した署名を付した検証情報ＳＣＡを携帯端末１を介してＩＣカード５Ａに送信する（Ｌ３）。

【００５５】ＩＣカード５Ａは、管理サーバ３から受信した検証情報ＳＣＡにおける署名を管理サーバ３の公開鍵ＫＥＹＰＣＡを用いて確認した後、受信した公開鍵「ＫＥＹＰ１」を用いてＩＣカード５Ｂからのアクセス要求Ｓ１における署名をチェックする。署名のチェック方法は任意であり、例えば管理サーバ３から取得した公開鍵で署名を復号化した結果が、要求情報のハッシュ値と合致するかを判別してもよい。

【００５６】ＩＣカード５Ａは、ＩＣカード５Ｂによる署名の正当性を確認すると、次に、管理サーバ３から取得したユーザＩＤ「ＵＩＤ１０」のアクセス情報を参照し、アクセス対象の「カルテ情報」について設定されているアクセス権限が、アクセスコマンドと合致するかを判別する。なお、この例において管理サーバ３が記憶するアクセス権限表は、例えば図２に示すアクセス権限表と同様の内容を有することとする。従って、グループＩＤ「ＧＩＤ１０」のアクセス情報の「カルテ情報」のアクセス権限は「読出」と「書込」の双方が許可されているため、カルテ情報の読み出しを要求するアクセスコマンドと合致すると判断される。

【００５７】ＩＣカード５Ｂからのアクセス要求Ｓ１における署名とアクセスコマンドのチェックが正常に完了すると、ＩＣカード５Ａは、アクセスコマンド「カルテ情報を読み出す」を実行し、実行結果をＩＣカード５Ｂに返す（Ｌ４）。この場合、ＩＣカード５Ａがメモリ５２から患者Ａのカルテ情報を読み出し、携帯端末１を介してＩＣカード５Ｂに送信する。そして、ＩＣカード５Ｂが、受信したカルテ情報を所定の表示要求とともに携帯端末１に送信して表示させる。また、ＩＣカード５ＡからＩＣカード５Ｂへは実行結果が正常である旨のＯＫ信号を送信し、カルテ情報は、ＩＣカード５Ａから携帯端末１へ所定の表示要求とともに送信されるようにしてもよい。これにより、医者Ｂが患者ＡのＩＣカード５Ａに記憶されるカルテ情報を読むことができる。

【００５８】なお、署名の認証とアクセスコマンドの検証の少なくとも一方がエラーとなった場合、ＩＣカード５Ａは、所定のエラー信号をＩＣカード５Ｂに送信する。また、アクセスコマンドを実行した際にエラーが発生した場合には、ＩＣカード５Ａは、実行結果として所定のエラー信号をＩＣカード５Ｂに送信する。

【００５９】患者Ａのカルテ情報を読み、患者Ａの診察を行った医者Ｂは、患者ＡのＩＣカード５Ａにアクセスして、患者Ａの診察結果をカルテ情報として記録しようとする。このカルテ情報を記録するための認証処理について図９を参照して説明する。

【００６０】例えば患者ＡのＩＣカード５Ａと医者ＢのＩＣカード５Ｂは、上記と同様に、携帯端末１の各カード挿入口にセットされていることとする。医者Ｂは、診察結果情報と、患者ＡのＩＣカード５Ａにカルテ情報を記録することの要求を入力する。携帯端末１は、この入力に応答して、診察結果情報と「カルテ情報を書き込む」というアクセスコマンドを、医者ＢのＩＣカード５Ｂに送信する。

【００６１】ＩＣカード５Ｂは、受信した診察結果情報、アクセスコマンド「カルテ情報を書き込む」、医者ＢのユーザＩＤ「ＵＩＤ１」及びグループＩＤ「ＧＩＤ１０」を含む要求情報に、自己の秘密鍵ＫＥＹＳ１を用いた署名を付与してアクセス要求Ｓ１を生成し、患者ＡのＩＣカード５Ａに携帯端末１を介して送信する（Ｌ１１）。

【００６２】患者ＡのＩＣカード５Ａは、ＩＣカード５Ｂからのアクセス要求Ｓ１を受信する。ＩＣカード５Ａは、先の認証処理（図８）で、ユーザＩＤ「ＵＩＤ１」に対応する公開鍵と、グループＩＤ「ＧＩＤ１０」に対応するアクセス情報を既に管理サーバ３から取得しているため、管理サーバ３に対するこれらの情報の要求は行わない。ＩＣカード５Ａは、ユーザＩＤ「ＵＩＤ１」に対応する公開鍵「ＫＥＹＰ１」を用いて署名をチェックし、また、グループＩＤ「ＧＩＤ１０」に対応するアクセス情報を用いてアクセスコマンドをチェックする。

【００６３】そして、ＩＣカード５Ｂからのアクセス要求Ｓ１における署名とアクセスコマンドのチェックが正常に完了すると、ＩＣカード５Ａは、ＩＣカード５Ｂから受信したデータ（診察結果情報）をカルテ情報としてメモリ５２記録することにより、アクセスコマンド「カルテを書き込む」を実行する。そして、実行結果（ＯＫ信号又はエラー信号）をＩＣカード５Ｂに返す（Ｌ１２）。これにより、医者Ｂは、認証を受けた後、患者Ａの診察結果を、患者ＡのＩＣカード５Ａに記録することができる。

【００６４】また、処方箋情報の記録も、上記のカルテ情報の記録と同様に処理される。この場合、ＩＣカード５Ｂからのアクセス要求は、医者ＢのユーザＩＤ、グループＩＤ、アクセスコマンド「処方箋情報を書き込む」、医者Ｂにより入力された処方箋情報等を含む。これにより、医者Ｂは、患者Ａに対する処方箋情報を患者ＡのＩＣカード５Ａに記憶させることができる。

【００６５】次に、患者Ａは、薬をもらうために薬局に行く。薬剤師Ｃが患者ＡのＩＣカード５Ａにアクセスして、カード内に記憶されている処方箋情報を読むために、薬剤師ＣのＩＣカード５Ｃが患者ＡのＩＣカード５Ａによる認証を受ける必要がある。この処方箋情報を読むための認証処理について説明する。

【００６６】まず、患者Ａは、自己のＩＣカード５Ａを、携帯端末１の第１の挿入口にセットする。また、薬剤師Ｃは、自己のＩＣカード５Ｃを、携帯端末１の第２の挿入口にセットし、例えば相手（患者Ａ）のＩＣカード５Ａに記憶されている処方箋情報を見ることの要求を入力する。携帯端末１は、この入力に応答して、「処方箋情報を読み出す」というアクセスコマンドを薬剤師ＣのＩＣカード５Ｃに送信する。

【００６７】これに応じて、ＩＣカード５Ｃは、受信したアクセスコマンド「カルテ情報を読み出す」と、例えばメモリ５２から読み出した薬剤師ＣのユーザＩＤ「ＵＩＤ２」及びグループＩＤ「ＧＩＤ２０」を含む要求情報と、この要求情報と自己の秘密鍵ＫＥＹＳ２を用いた署名を生成する。そして、図１０に示すように、ＩＣカード５Ｃは、要求情報に署名を付与したアクセス要求Ｓ２を、患者ＡのＩＣカード５Ａに携帯端末１を介して送信する（Ｌ２１）。

【００６８】患者ＡのＩＣカード５Ａは、ＩＣカード５Ｃからのアクセス要求Ｓ２の受信に応答し、例えばアクセス要求Ｓ２における要求情報に含まれるユーザＩＤ「ＵＩＤ２」に対する公開鍵と、グループＩＤ「ＧＩＤ２０」に対するアクセス情報とが未取得であることをメモリ５２を参照して確認した後、ユーザＩＤ「ＵＩＤ２」とグループＩＤ「ＧＩＤ２０」を含む検証情報要求を、携帯端末１を介して管理サーバ３に送信する（Ｌ２２）。

【００６９】管理サーバ３は、受信したユーザＩＤ「２」に対応する公開鍵「ＫＥＹＰ２」と、受信したグループＩＤ「ＧＩＤ２０」に対応するアクセス情報と、を記憶部３１から読み出し、これらの情報に、管理サーバ３の秘密鍵ＫＥＹＳＣＡを用いて生成した署名を付した検証情報ＳＣＡを携帯端末１を介してＩＣカード５Ａに送信する（Ｌ２３）。

【００７０】ＩＣカード５Ａは、管理サーバ３から受信した検証情報ＳＣＡにおける署名を管理サーバ３の公開鍵ＫＥＹＰＣＡを用いて確認した後、ユーザＩＤ「ＵＩＤ２」に対応する公開鍵「ＫＥＹＰ２」を用いてアクセス要求Ｓ２における署名の正当性をチェックする。また、グループＩＤ「ＧＩＤ２０」のアクセス情報を参照して、アクセス対象の「処方箋情報」について設定されているアクセス権限が、アクセスコマンドと合致するかをチェックする。なお、この例においても管理サーバ３が記憶するアクセス権限表は、例えば図２に示すアクセス権限表と同様の内容とする。従って、グループＩＤ「ＧＩＤ２０」のアクセス情報の「処方箋情報」についてはアクセス権限が何ら許可されておらず、アクセスコマンド」とは合致しない。この場合、ＩＣカード５Ａ

は、アクセス権限エラーを示すエラー信号をＩＣカード５Ｃに送信する。

【００７１】このようにアクセス要求がエラーとなった場合、患者Ａは、薬剤師Ｃが処方箋情報を見ることができるように薬剤師Ｃの権限を変更することができる。この場合、患者Ａは、例えばＰＩＮの入力チェックにより本人確認を行ったのち、所定グループのアクセス情報を追加変更する要求と、変更対象である薬剤師ＣのグループＩＤ「ＧＩＤ２０」と、追加したいコマンド「処方箋情報を読み出す」と、を入力し、携帯端末１は、入力された情報をＩＣカード５Ａに送信する。なお、薬剤師Ｃのグループの指定方法は任意であり、例えば上記のようにアクセス権限のチェックでエラーが発生した後に本処理を続行する場合には、エラーとなったグループのグループＩＤがＩＣカード５Ａ内で自動的に設定されてもよい。

【００７２】ＩＣカード５Ａは、図１１に示すように、薬剤師ＣのグループＩＤ「ＧＩＤ２０」、追加対象コマンド「処方箋情報を読み出す」等を含む権限追加要求を管理サーバ３に送信する（Ｌ３１）。管理サーバ３は、権限追加要求を受信すると、受信したグループＩＤ「ＧＩＤ２０」のアクセス情報を記憶部３１のアクセス権限表から読み出して、所定記憶領域等コピーする。そして、その読み出したアクセス情報に対して、コマンド「処方箋情報を読み出す」の追加処理を行う。そして、コマンドが追加された新たなアクセス情報に、管理サーバ３の秘密鍵ＫＥＹＳＣＡを用いた署名を付してＩＣカード５Ａに送信する（Ｌ３２）。なお、このとき、記憶部３１に記憶されるアクセス権限表のアクセス情報は更新しない。

【００７３】ＩＣカード５Ａは、アクセス権限が追加変更されたグループＩＤ「ＧＩＤ２０」を受信してメモリ５２に記憶する。これにより、患者ＡのＩＣカード５Ａに記憶される薬剤師Ｃのアクセス権限が変更される。

【００７４】なお、ＩＣカード５Ａが管理サーバ３にグループＩＤ「ＧＩＤ２０」のアクセス権限変更のための書換命令発効依頼を送信し、管理サーバ３がこれに応じて、「ＧＩＤ２０」のアクセス情報についての書換命令をＩＣカード５に送信し、これに応じて、ＩＣカード５Ａがメモリ５２に記憶されている「ＧＩＤ２０」のアクセス情報を書き換えるようにしてもよい。

【００７５】次に、アクセス権限が変更された薬剤師ＣはＩＣカード５Ａに記憶されている処方箋情報を見ることの要求を入力する。携帯端末１は、この入力された「処方箋情報を読み出す」というアクセスコマンドをＩＣカード５Ｃに対して送信する。これに応答して、ＩＣカード５Ｃは、図１２に示すように、アクセスコマンド「処方箋情報を読み出す」、薬剤師ＣのユーザＩＤ「ＵＩＤ２」及びグループＩＤ「ＧＩＤ２０」を含む要求情報に、自己の秘密鍵ＫＥＹＳ２を用いた署名を付与してアクセス要求Ｓ２を生成し、患者ＡのＩＣカード５Ａに携帯端末１を介して送信する（Ｌ４１）。

【００７６】患者ＡのＩＣカード５Ａは、ＩＣカード５Ｃからのアクセス要求Ｓ２を受信する。ＩＣカード５Ｃは、先の認証処理及びアクセス権限変更処理（図１０、図１１）で、ユーザＩＤ「ＵＩＤ２」に対応する公開鍵と、グループＩＤ「ＧＩＤ２０」の変更後のアクセス情報を既に取得しているため、管理サーバ３に対するこれらの情報の要求は行わない。ＩＣカード５Ａは、ユーザＩＤ「ＵＩＤ２」に対応する公開鍵「ＫＥＹＰ２」を用いて署名をチェックし、また、グループＩＤ「ＧＩＤ２０」のアクセス情報を参照して、「処方箋情報」について設定されているアクセス権限が、アクセスコマンドと合致するかをチェックする。この場合、アクセス情報に「処方箋情報を読み出す」旨のアクセス権限が追加されたため、チェック結果は正常を示す。

【００７７】そして、ＩＣカード５Ｃからのアクセス要求Ｓ２における署名とアクセスコマンドのチェックが正常に完了すると、ＩＣカード５Ａは、アクセスコマンド「処方箋情報を読み出す」を実行し、実行結果をＩＣカード５Ｃに返す（Ｌ４２）。例えば、ＩＣカード５Ａがメモリ５２から患者Ａの処方箋情報を読み出し、携帯端末１を介してＩＣカード５Ｃに送信する。そして、ＩＣカード５Ｃが、受信した処方箋情報を所定の表示要求とともに携帯端末１に送信して表示させる。また、ＩＣカード５ＡからＩＣカード５Ｃへは実行結果が正常である旨のＯＫ信号を送信し、処方箋情報は、ＩＣカード５Ａから携帯端末１へ所定の表示要求とともに送信されるようにしてもよい。これにより、薬剤師Ｃのアクセス権限の変更を行って、患者ＡのＩＣカード５Ａに記憶される処方箋情報を薬剤師Ｃが読むことができる。

【００７８】なお、薬剤師Ｃについて追加したアクセス権限が今後必要ない場合には、ＩＣカード５Ａが、コマンド「処方箋情報を読み出す」の削除を要求する権限変更要求を管理サーバ３に送信してコマンドの削除を行ってもよい。また、削除せずにこのままにしておけば、以後もオフラインで薬剤師ＣのＩＣカード５Ｃの検証が可能となる。

【００７９】このようにして、全ＩＣカード５の認証用の鍵（公開鍵）やアクセス権限の情報を管理サーバ３で集中管理し、各ＩＣカード５は、相手の認証に必要な情報（公開鍵、アクセス情報）を管理サーバ３から取得して認証チェックを行う。これにより、ＩＣカードに大容量のメモリを必要とすることなく、ＩＣカードの資源を効率良く使用できる。また、システムにおけるＩＣカード側の負担を軽減した認証システムを実現することができる。また、システムの安全性及びメンテナンス性を向上することができる。

【００８０】また、上記説明では、カード保持者が、自己のＩＣカード５に記憶するアクセス情報について、各

グループに付与されているアクセス権限を変更することができるようにしているが、例えばカルテ情報等のように大事なデータは第三者（カルテ情報であれば医者等）の署名をつけて利用者（患者）のＩＣカード５に記憶させるようにして、データの書換を防止してもよい。また、利用者からの要求により、各利用者のＩＣカード５から管理サーバ３に依頼した命令（要求）等はログを取ることができるようにしてもよい。そして、取ったログを不正使用の調査等に用いてもよい。

【００８１】また、ＩＣカード５間の通信手段となる携帯端末１及びネットワーク７の使用形態は任意である。例えば、患者が病院で検査を受けて、その数日後に検査結果を受け取る場合に、検査結果を示すカルテ情報と処方箋情報を、自宅や職場等の任意の場所で、有線又は無線通信により携帯端末１で受信し、患者のＩＣカード５に記録することもできる。この場合、例えば医者のＩＣカード５から患者のＩＣカード５へのアクセス要求が所定サーバに格納され、患者が携帯端末１から所定サーバにアクセスして自己宛のアクセス要求を取得する。所定サーバが、アクセス要求が登録されたことを検出して、所定の宛先に、登録されたアクセス要求を送信してもよく、又、アクセス要求が登録されたことの通知を送信してもよい。患者のＩＣカード５は、上記説明と同様にして、取得したアクセス要求について署名及びアクセス権限の認証を行った後、ＩＣカード５に検査結果を示すカルテ情報や処方箋情報を記録する。

【００８２】そして、ＩＣカード５に記録された処方箋情報のみを薬局から遠隔的にアクセスさせて、薬を患者に送付してもらうようにしてもよい。患者の処方箋情報をアクセスする処理を自動化して、薬の販売が２４時間可能な自動販売機や薬販売受付サービスを実現してもよい。また、患者が、自分で体重、血圧等の測定を行い、測定情報を病院に送信し、病院側で患者の認証を行った後、検査、分析等に用いてもよい。無線通信機能を備える携帯端末（携帯電話機）を用いることにより、患者は外出先等でも検査結果を示すカルテ情報や処方箋情報を受け取ることができ、その利用場所が制限されることがないため、利便性はさらに向上する。

【００８３】また、上記説明ではアクセス要求元の認証処理をＩＣカード５内で行っていたが、この認証機能を管理サーバ３にも持たせても良い。この場合、他のＩＣカード５からのアクセス要求を受信したＩＣカード５は、受信したアクセス要求を管理サーバ３に送信する。管理サーバ３は、受信したアクセス要求に含まれるユーザＩＤとグループＩＤに対応する公開鍵とアクセス情報を記憶部３１から読み出し、ＩＣカード５による認証処理と同様にして、アクセス要求に含まれる署名とアクセスコマンドをチェックし、チェック結果をＩＣカード５に送信する。ＩＣカード５は、管理サーバ３からのチェック結果が正常を示す場合には、アクセスコマンドを実行し、チェック結果がエラーである場合には、エラー信号をアクセス要求元に返す。

【００８４】また、上記説明では、アクセス対象となる情報（個人情報）を記憶するＩＣカード５と、ＩＣカードの通信手段となる携帯端末１とを用いるようにしているが、これに限定されず、ＩＣカード５を用いずに、上記のＩＣカード５の機能をさらに有する携帯端末１を用いてもよい。この場合、携帯端末１は、例えば、上記説明においてＩＣカード５に記憶されていた秘密鍵及び公開鍵、個人情報等を記憶部１５に記憶し、アクセス要求の作成・送受信、アクセス要求元の認証、管理サーバ３との送受信、アクセスコマンドの実行等を行う。

【００８５】ＩＣカード５と管理サーバ３との間の通信は、安全上、暗号を用いることが望ましい。例えば、ＩＣカード５が乱数を発生させ、この乱数を他の情報とともに管理サーバ３に送信し、管理サーバ３が署名対象の情報にＩＣカード５から受信した乱数を含めて署名を行い、ＩＣカード５が管理サーバ３から受信した署名に含まれる乱数を確認するようにしてもよい。これにより、割り込みによる偽メッセージの送受信を防ぐことができる。

【００８６】また、本システムは、病院用の認証システムに限定されず、例えば電子マネーを記憶するＩＣカードを用いる電子マネーシステム、個人情報を記憶するＩＣカードを用いて住民票の発行等の行政サービスを行う行政システム等、認証処理を行う種々のシステムに適用され得る。

【００８７】また、本発明を用いて、例えば、ＩＣカードにコンテンツを格納し、インターネット上のホームページにアクセスするのと同様に、ＩＣカードに格納されたコンテンツにアクセスするシステムを実現してもよい。例えば、利用者Ａが利用者ＢのＩＣカードに格納されているコンテンツを見たい場合には、利用者Ａは携帯端末等に自己のＩＣカードをセットして、利用者ＢのＩＣカードに対してアクセス要求を送信する。利用者Ｂの端末は、利用者ＡのＩＣカードからのアクセス要求を受信すると、上記説明と同様にして、署名及びアクセス権限をチェックし、チェック結果が正常を示せばアクセスを許可し、利用者Ａは、利用者Ｂのコンテンツを例えばダウンロードすることができる。これにより、従来のインターネットシステムにおけるコンテンツを管理するＷＷＷサーバ等を必要とすることなく、携帯端末とＩＣカード等の簡易な構成でネットワークを介した情報提供サービスを実現することができる。この場合、例えば複数の回線を使用する等して、複数の利用者からのアクセス要求を受け付け可能としてもよい。また、アクセス者からの要求に応じて、コンテンツ提供者がそのアクセス者と会話できるようにしてもよい。この場合、例えば、アクセス要求元から所定の通話要求の受信に応じて、携帯電話機等のデータ送受信モードを通話モードに切り換え

て、所定のデータ送受信の手続に従って音声データを送受信する。

【００８８】なお、ＩＣカード５に記憶されるコンテンツ等を所定の鍵で暗号化しておき、管理センタ３からアクセスＯＫの指令が出たとき、又は、カード内で認証結果が確認されたとき、管理センタ３からのコンテンツ復号用の鍵を受け取って、アクセス対象のデータを復号化してもよい。

【００８９】なお、この発明のＩＣカード認証システムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行する携帯端末１、管理サーバ３等を構成することができる。なお、上述の機能を、ＯＳが分担又はＯＳとアプリケーションの共同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納してもよい。

【００９０】なお、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００９１】

【発明の効果】以上説明したように、本発明によれば、ＩＣカード等の認証用鍵等をサーバで集中管理して、あるＩＣカード等にアクセス要求があった場合には、相手の認証に必要な情報をサーバから取得して認証処理を行う。これにより、多数の認証用鍵やアクセス情報を記憶するための大容量のメモリを必要とせずに資源を効率良く使用でき、記憶容量に基づくシステムの利用制限を軽減することができる。また、システムの安全性を保持しつつ、システムにおけるＩＣカード側の負担等を軽減することができる。

【図面の簡単な説明】

＊【図１】本発明の実施の形態に係るＩＣカード認証システムのシステム構成図である。

【図２】図１のＩＣカード認証システムで使用される携帯端末の構成を説明するための図である。

【図３】図１のＩＣカード認証システムで使用される管理サーバの構成を説明するための図である。

【図４】アクセス権限表を説明するための図である。

【図５】ＩＣカードの構造を説明するための図である。

【図６】ＩＣカードに記憶される初期情報と個人情報を説明するための図である。

【図７】ＩＣカードに記憶される公開鍵とアクセス情報を説明するための図である。

【図８】患者のＩＣカードが医者のＩＣカードを認証する場合の処理を説明するための図である。

【図９】患者のＩＣカードが医者のＩＣカードを認証する場合の処理を説明するための図である。

【図１０】患者のＩＣカードが薬剤師のＩＣカードを認証する場合の処理を説明するための図である。

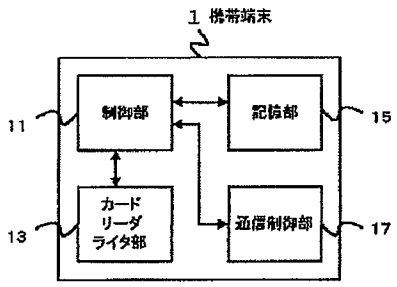
【図１１】患者のＩＣカードが薬剤師のアクセス権限を変更する場合の処理を説明するための図である。

【図１２】患者のＩＣカードが薬剤師のＩＣカードを認証する場合の処理を説明するための図である。

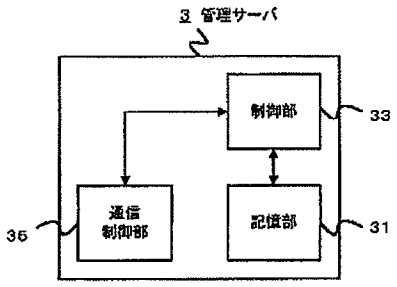
【符号の説明】

１	携帯端末
１１	制御部
１３	カードリーダライタ部
１５	記憶部
１７	通信制御部
３	管理サーバ
３１	記憶部
３３	制御部
３５	通信制御部
５	ＩＣカード
５１	制御部
５２	メモリ
５３	入出力制御部
７	ネットワーク

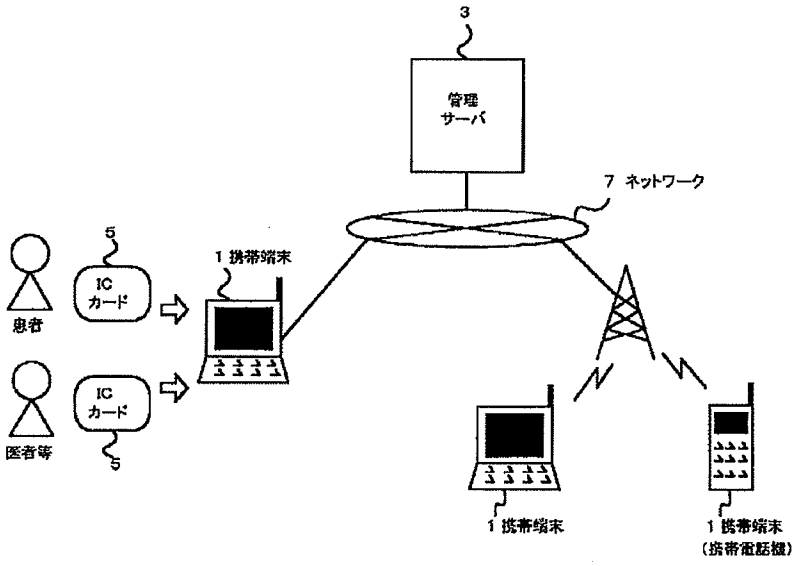
【図２】



【図３】



【図１】

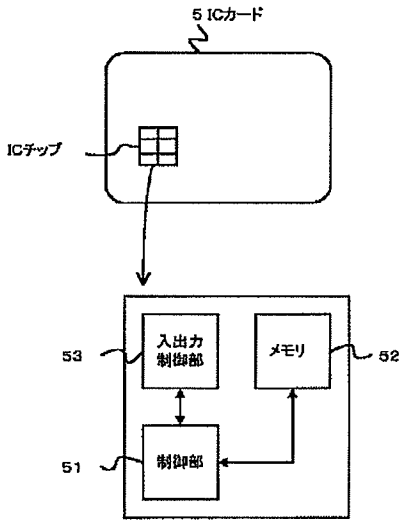


【図４】

アクセス権限表

グループID	アクセス情報	
GID10 （医者）	名前情報	読出可
	住所情報	読出可
	カルテ情報	読出／書込可
	処方箋情報	読出／書込可
	・ ・ ・	・ ・ ・
GID20 （薬剤師）	名前情報	読出可
	住所情報	読出可
	カルテ情報	－
	処方箋情報	－
	・ ・ ・	・ ・ ・
・ ・ ・	・ ・ ・	・ ・ ・

【図５】



【図６】

(A)

初期情報

秘密鍵
公開鍵
ユーザID
グループID
管理サーバの公開鍵
・・・

(B)

個人情報

名前情報
住所情報
カルテ情報
処方箋情報
・・・

【図７】

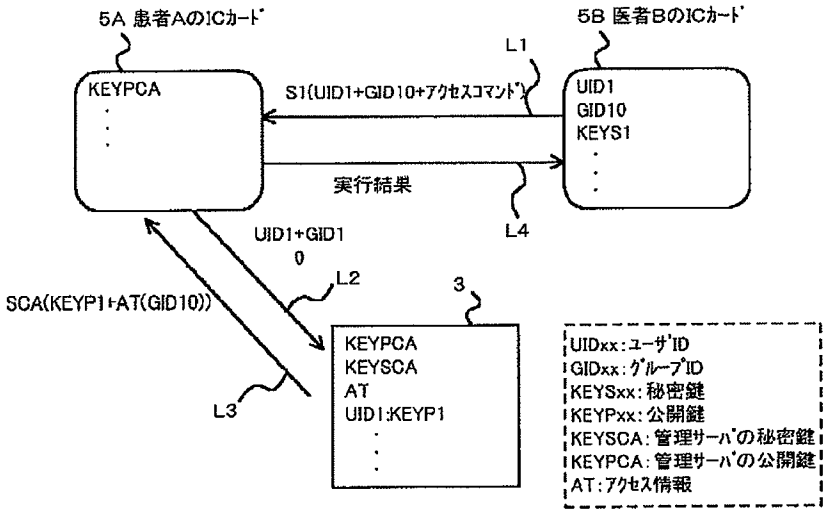
(A)

ユーザID	公開鍵
XXXXXXX	XXXXXXX
・・・	・・・

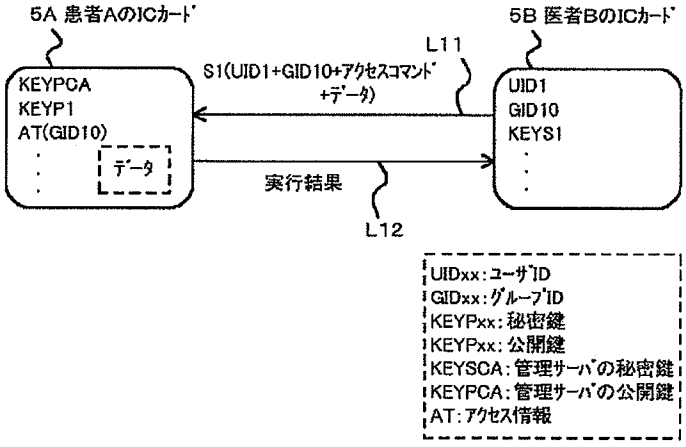
(B)

グループID	アクセス情報	
GID10	名前情報	読出可
	住所情報	読出可
	カルテ情報	読出／書込可
	処方箋情報	読出／書込可
	・・・	・・・
・・・	・・・	・・・

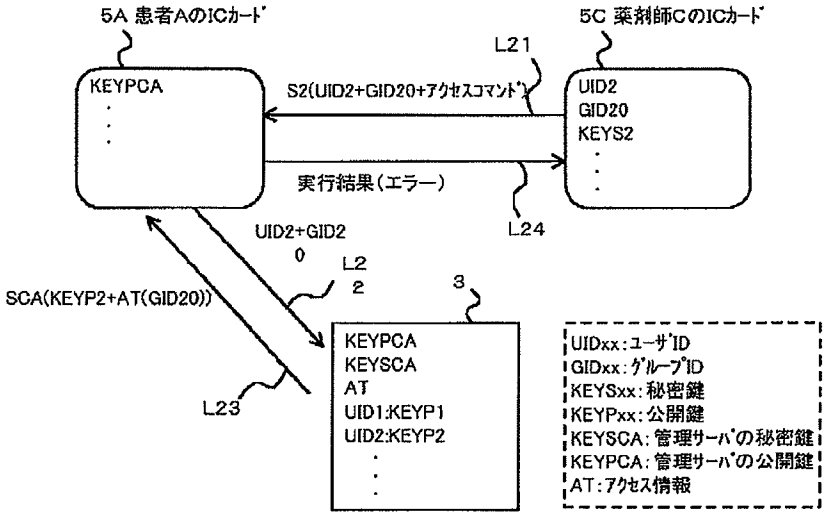
【図８】



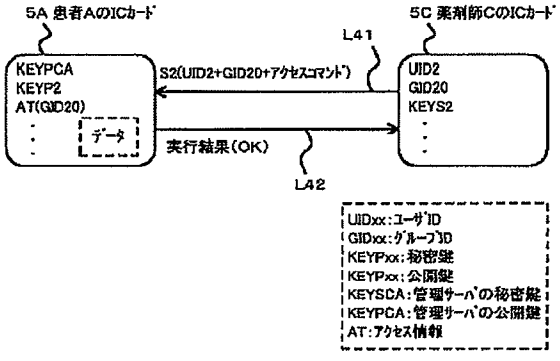
【図９】


5A 患者AのICカード
5B 医者BのICカード
L11
S1(UID1+GID10+アクセスコマンド+データ)
KEYPCA
KEYP1
AT(GID10)
データ
UID1
GID10
KEYS1
実行結果
L12
UIDxx:ユーザID
GIDxx:グループID
KEYPxx:秘密鍵
KEYPxx:公開鍵
KEYSCA:管理サーバの秘密鍵
KEYPCA:管理サーバの公開鍵
AT:アクセス情報

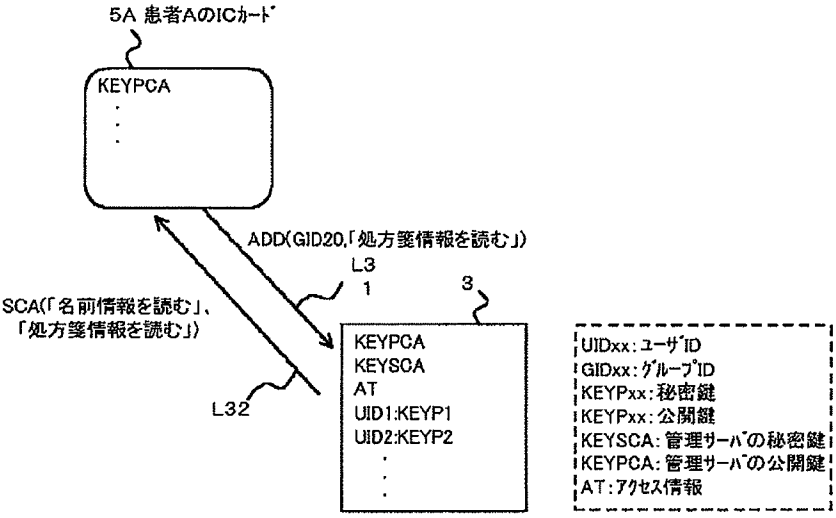
【図１０】


5A 患者AのICカード
5C 薬剤師CのICカード
L21
KEYPCA
S2(UID2+GID20+アクセスコマンド)
UID2
GID20
KEYS2
実行結果(エラー)
L24
UID2+GID2
0
L2
2
3
SCA(KEYP2+AT(GID20))
L23
KEYPCA
KEYSCA
AT
UID1:KEYP1
UID2:KEYP2
UIDxx:ユーザID
GIDxx:グループID
KEYSxx:秘密鍵
KEYPxx:公開鍵
KEYSCA:管理サーバの秘密鍵
KEYPCA:管理サーバの公開鍵
AT:アクセス情報

【図１２】


5A 患者AのICカード
5C 薬剤師CのICカード
L41
KEYPCA
KEYP2
AT(GID20)
データ
S2(UID2+GID20+アクセスコマンド)
UID2
GID20
KEYS2
実行結果(OK)
L42
UIDxx:ユーザID
GIDxx:グループID
KEYPxx:秘密鍵
KEYPxx:公開鍵
KEYSCA:管理サーバの秘密鍵
KEYPCA:管理サーバの公開鍵
AT:アクセス情報

【図１１】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｋ	19/00	Ｐ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ

(72)発明者　町田　修
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考)　5B035 AA00 BB09 BC01 CA38
5B058 CA27 KA02 KA04 KA33 YA20
5B085 AE12 AE13 AE23 BG07
5J104 AA07 AA09 AA12 EA26 KA02
KA05 LA03 LA06 MA02 MA06
NA02 NA20 NA35 NA36 NA40
PA07
9A001 BB05 EE03 JZ25 JZ27 KZ58
KZ60 KZ61 LL03